U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

US-APWR I&C Design Certification

Technical Report
&
Design Control Document References Review

Royce D. Beacom
Instrumentation, Controls and Electrical Engineering Branch (ICE1)
Office of New Reactors

Michael D. Muhlheim, Ph.D
Oak Ridge National Laboratory

Thomas L. Wilson, Ph.D
Oak Ridge National Laboratory

Wednesday, February 3, 2010

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Purpose

- Status of Safety I&C Topical Report & Referenced Reports
- Status of MELTAC Topical Report & Referenced Reports
- Software Program Manuals &
  - Branch Technical Position 7-14
- Status of DCD Review & Referenced Reports

Non-Proprietary

Safety I&C System Description & Design Process

Does not contain sufficient information to make a safety determination for Operating Reactors:

- NRR is not reviewing these references:
  - MUAP-07005 MELTAC
  - MUAP-07006 Defense-in-Depth and Diversity
  - MUAP-07007 HSI Sys Description & HFE Process
  - MUAP-08003 Cyber Security Program
  - US-APWR Design Control Document

All are referenced in the review of Safety I&C System Topical Report

Safety I&C System Description & Design Process

NRO is recommending the report be withdrawn and resubmitted as a Technical Report:

- The report now is applicable only to US-APWR.
- Technical issues could be resolved according to the DCD review schedule not as application specific in a Topical Report Safety Evaluation.
- Many subjects currently in the report are more thoroughly presented in the US-APWR Design Certification.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Safety I&C System Description and Design Process

These are the Technical Issues with this Topical Report:

- Credited manual safety functions must have priority over non-safety controls at all times:
  - Section 4.2.4(b); States "Safety VDUs are backup controls"
    - However, the safety VDUs are the credited VDUs for design basis events. This should be stated in the report.
  - Section 4.2.5(c); Acceptable safety function performance conflicts; "Safety VDU can have priority ..."

Safety I&C System Description and Design Process

- Control Priority Logic
  - Figure 5.1-3 indicates a generic provision for automatic non-safety start and stop demands.
  - No specific use of these functions is given in the Topical Report
  - Determination of IEEE Std 7-4.3.2 and ISG-04 compliance is based on no unused resident functions. Specific usage and justification should be identified in the application.

Safety I&C System Description and Design Process

- Modifiable Priority Logic
  - Nonvolatile memory should be changeable only through a removable memory device.
    - ISG 04, Staff Position 2, Point 7
  - Section 3.5.1.2, the logic that prioritizes the signals from the Operational VDU and PSMS is contained in the PSMS application Software that is stored in the nonvolatile F-ROM which may be reprogrammed while in the CPU module.

Non-Proprietary

Safety I&C System Description and Design Process

- Can the Completion of Protection Action be done with the override feature ?
  - Section 4.2.2; states "some functions" may be overridden
    - What are those functions?

- The Engineering Tool is described as off-line
  - (see MELTAC Engineering Tool discussion)

Safety I&C System Description and Design Process & MELTAC Reports

- Branch Technical Position 18; Guidance on use of PLC in Digital Computer based I&C Systems
- NUREG 6421; Guidance for proposed acceptance process for COTS software –
- *Are* applicable:

Safety I&C System Description and Design Process & MELTAC Reports

- The issue is: Is this a 10 CFR 50 Appendix B program?
  - Not the application it was originally designed for.
- If it is not from an Appendix B program, it is a commercial dedication. These documents then apply.
  - MELTAC platform will be a commercial dedication.

Safety I&C System Description and Design Process

- The FMEA methodology is not reflected in the application MUAP-09020 (Discussed later)
- Time response method is not reflected in the application MUAP-09021 (Discussed later)
- The overall I&C System Architecture states the DAS is hardwired or *digital*.
  - Conflicts with D3 Topical Report and Safety Evaluation.
  - Issue identified in RAI-5 but not adequately resolved.

Safety I&C System Description and Design Process

- Credit for self diagnostics for Tech Spec Surveillances
    - From 22, 23 Jan. 08' Meeting:
        - History of Self-diagnostics has not been provided.
    - Response to RAI-63 should be completed; Including what surveillances are no longer necessary because of self- diagnostics.
- Credit for Leak Detection
    - Not Applicable; See Safety Evaluation for D3.

Safety I&C System Description and Design Process

- Sections 6.1 through 6.4 of the Design Process does not provide a level of detail, relative to the licensing guidance, for the staff to make a safety determination on the Design or Life Cycle process.
  - The staff uses Branch Technical Position 7-14, Guidance on Software Reviews for Digital Computer-Based I&C.
  - The staff also uses the 6 software related Regulatory Guides 1.168 – 1.173.
  - The descriptive text is informative but the staff cannot approve it as meeting the BTP 7-14 or the Reg. Guides.

Non-Proprietary

Safety I&C System Description and Design Process

- Section 6.5.4, Accuracy Analysis Method, does not provide a level of detail, relative to the licensing guidance, for the staff to make a reasonable safety determination on this process.
  - The staff uses Branch Technical Position 7-12 *and* RG 1.105. (Compliance to 7-12 cannot be "see RG 1.105")
  - RAI 71 response should be completed by referencing the points the staff raised within the new setpoint methodology document, MUAP-09022.

Safety I&C System Description and Design Process

– Control system failure modes for Safety Analysis.

- Appendix C, Malfunctions and spurious commands, states *three* operator commands are required to generate commands to plant equipment from the Operational VDU.
- MUAP-07007 (HSI) and the Software Safety Analysis state that the Operational VDU and Safety VDU are designed such that *two* distinct actions are required to initiate any control action.

Safety I&C System Description and Design Process

– Multi-channel operator stations.

- Commands for multiple, simultaneous, erroneous actions by the Operating VDU are considered credible unless an extraordinarily clear demonstration of low probability can be made.
- Appendix C does not address the possibility of a single common mode software error which results in all three requirements for failure to detect an erroneous command are satisfied.

Safety I&C System Description and Design Process

– Multi-channel operator stations.

- The measures cited are valid and useful for correctness of data and provide high degree of protection from a communication that is corrupted by noise.
- ISG-04 requires all of these potential corruptions of messages in Position 1 Point 12 to be addressed as part of the communication software design.

Safety I&C System Description and Design Process

– Multi-channel operator stations.

- The ISG-04 requirement does not suggest that a potential failure of the system to identify correctly and block them could not exist and should be satisfactorily prevented from adverse consequences in the safety system as required by single failure criterion of IEEE Std 379.
- Therefore, RAIs 54, with regards to valid but erroneous commands, and 55, on the VDU enhanced QA program, should be revisited.

Safety I&C System Description and Design Process

- These subjects are discussed elsewhere US-APWR therefore review by the staff would not be included within the scope of Safety Evaluation (if it was a topical report);
  - Reliability Method (PRA & Plant Licensing Document
  - Seismic Analysis Method (US-APWR DCD)
  - EMI Analysis Method (MELTAC Topical Report)
  - Fire Protection Analysis (US-APWR DCD)

Safety I&C System Description and Design Process

- Integrated RPS/ESFAS with functional diversity (In the D3 Safety Evaluation)
- CCF Failure Modes for D3 Analysis
  - In the D3 Safety Evaluation
- HSI to accommodate reduced staffing
  - HSI Topical Report

Safety I&C System Description and Design Process

- Minimum Inventory of HSI
  - HSI Topical Report & Plant Licensing Doc
- Computer Based Procedures
  - HSI Topical Report

Safety I&C System Description and Design Process

- Common output modules for PSMS/PCMS and DAS
  - MELTAC Topical Report
- Credit for self-diagnostics for TS surveillances
  - Should be part of MELTAC Topical Report
  - See Technical Problem on history and what surveillances are no longer necessary

US-APWR Functional Assignment Analysis for Safety Logic System Report

- Does not refer back to MUAP-07004.
- Does not provide a reference section.
- Ch. 7 in MUAP-07004 indicates that the FMEA will be provided as Plant Licensing Documentation.
- However, RAI 07.03-8 states that the “FMEA report will be submitted by September 2009.” Is this MUAP-09020?

US-APWR Functional Assignment Analysis for Safety Logic System Report

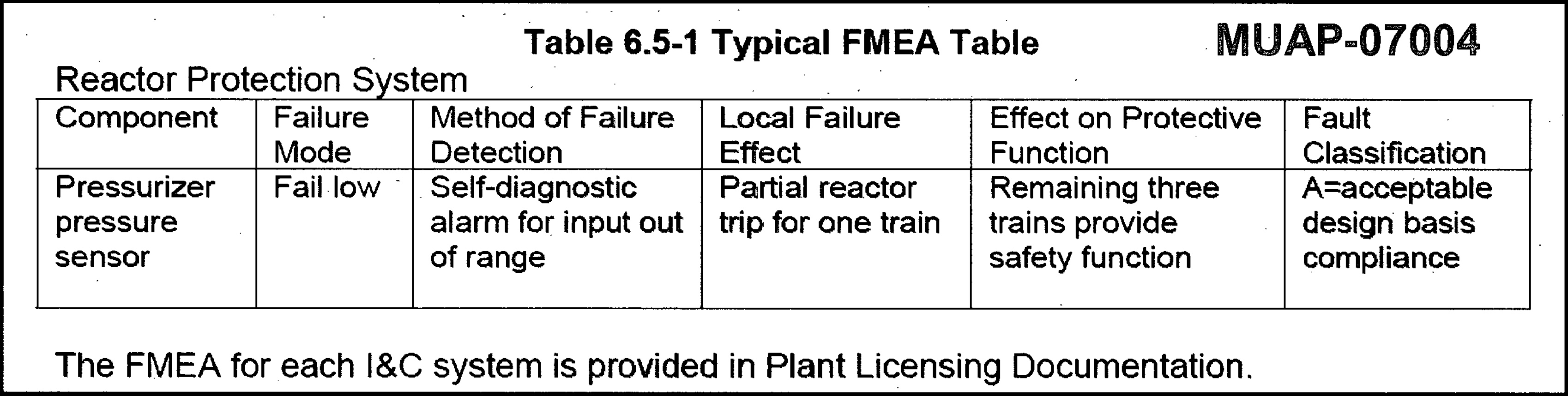


Table 6.5-1 Typical FMEA Table **MUAP-07004**

Reactor Protection System

Component	Failure Mode	Method of Failure Detection	Local Failure Effect	Effect on Protective Function	Fault Classification
Pressurizer pressure sensor	Fail low	Self-diagnostic alarm for input out of range	Partial reactor trip for one train	Remaining three trains provide safety function	A=acceptable design basis compliance

The FMEA for each I&C system is provided in Plant Licensing Documentation.

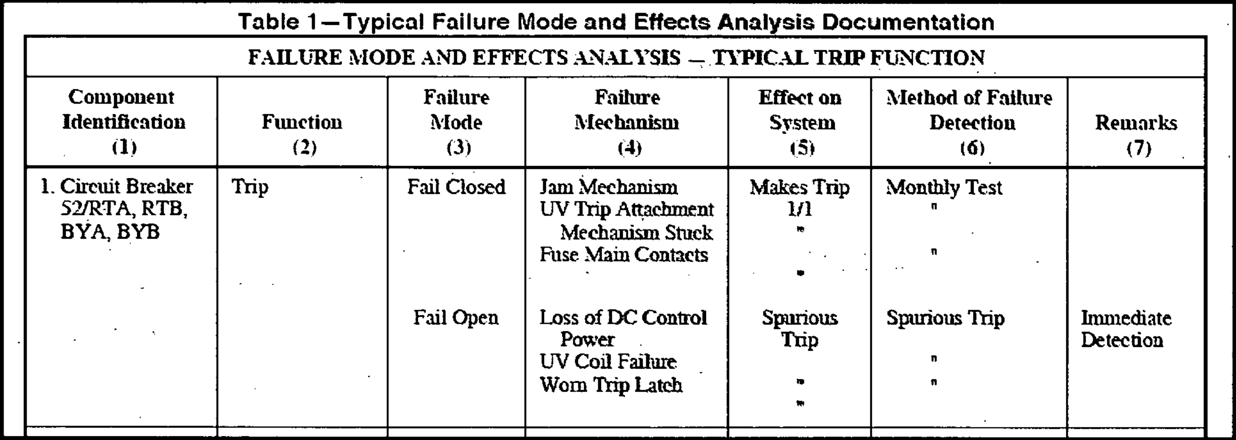


Table 1—Typical Failure Mode and Effects Analysis Documentation

FAILURE MODE AND EFFECTS ANALYSIS — TYPICAL TRIP FUNCTION

Component Identification (1)	Function (2)	Failure Mode (3)	Failure Mechanism (4)	Effect on System (5)	Method of Failure Detection (6)	Remarks (7)
1. Circuit Breaker 52/RTA, RTB, BYA, BYB	Trip	Fail Closed	Jam Mechanism	Makes Trip 1/1	Monthly Test	
			UV Trip Attachment Mechanism Stuck	"	"	
			Fuse Main Contacts	"	"	
		Fail Open	Loss of DC Control Power	Spurious Trip	Spurious Trip	Immediate Detection
			UV Coil Failure	"	"	
			Worn Trip Latch	"	"	
				"		

IEEE Std 352- 1987

US-APWR Functional Assignment Analysis for Safety Logic System Report

MUAP-07020

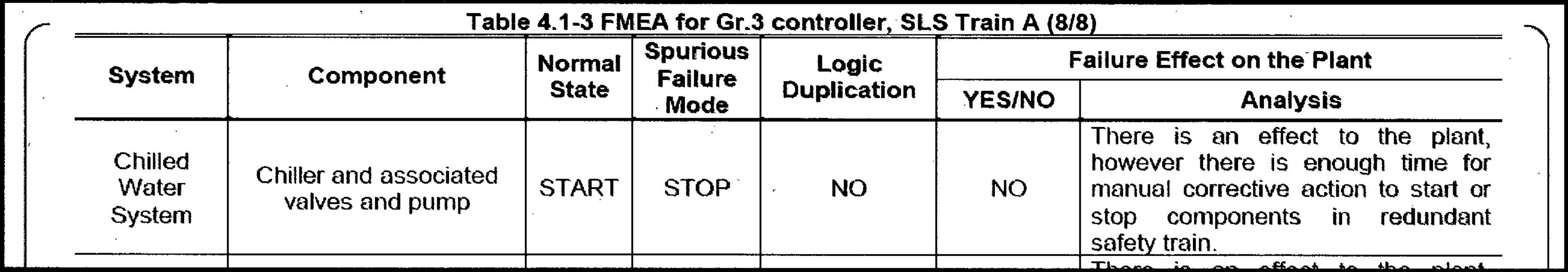


Table 4.1-3 FMEA for Gr.3 controller, SLS Train A (8/8)

System	Component	Normal State	Spurious Failure Mode	Logic Duplication	Failure Effect on the Plant	
					YES/NO	Analysis
Chilled Water System	Chiller and associated valves and pump	START	STOP	NO	NO	There is an effect to the plant, however there is enough time for manual corrective action to start or stop components in redundant safety train.
						There is an effect to the plant

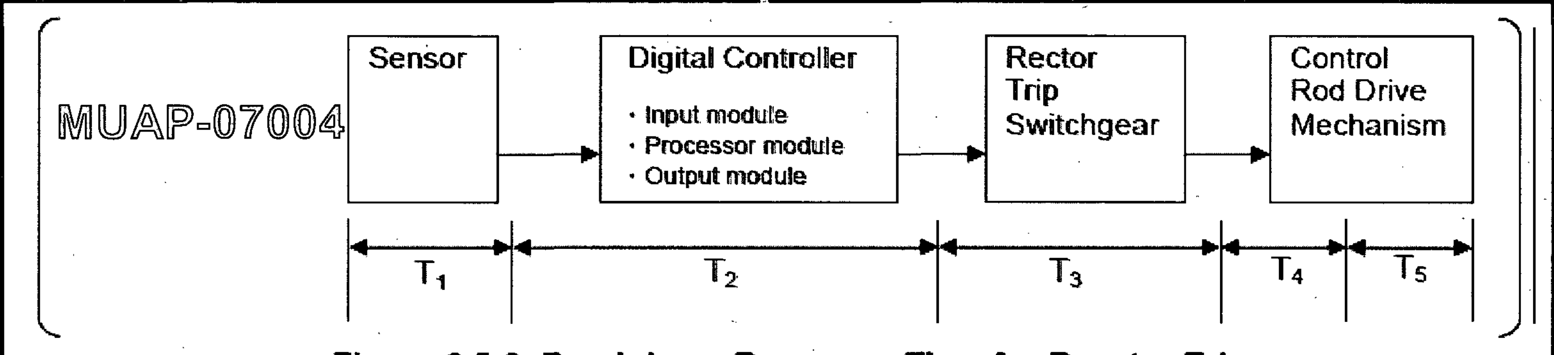
- Does not follow IEEE standards and does not evaluate I&C component failures or identify the modes of these failures, and the effects of these failures
- Suggest revision of this technical report and resubmit for review

US-APWR Response Time of Safety I&C System Report

- The response time calculation formula in MUAP-07004 does not match that in MUAP-09021.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

US-APWR Response Time of Safety I&C System Report



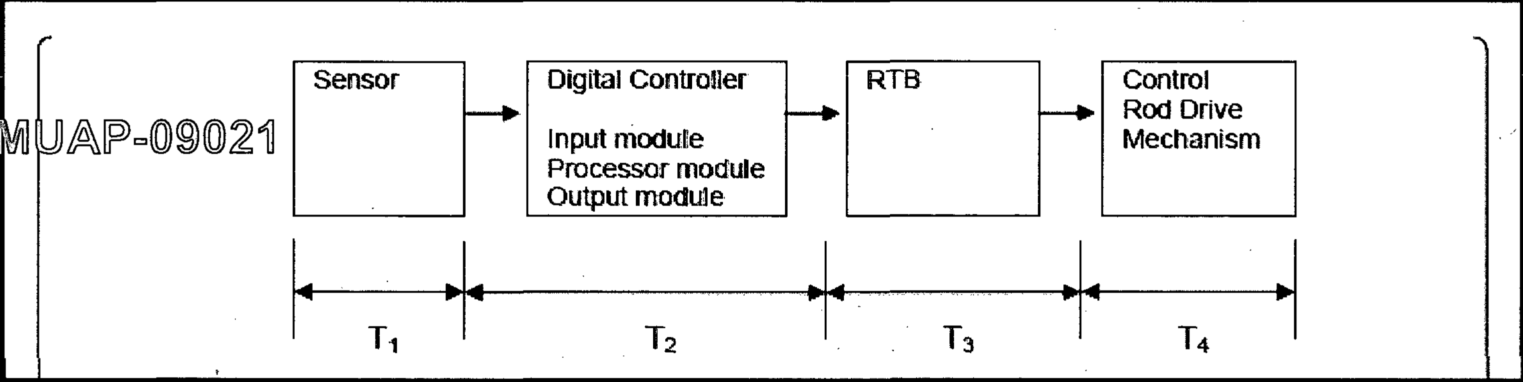
MUAP-07004

Sensor → Digital Controller
- Input module
- Processor module
- Output module

→ Rector Trip Switchgear → Control Rod Drive Mechanism

T_1 T_2 T_3 T_4 T_5

Figure 6.5-2 Breakdown Response Time for Reactor Trip



MUAP-09021

Sensor → Digital Controller

Input module
Processor module
Output module

→ RTB → Control Rod Drive Mechanism

T_1 T_2 T_3 T_4

MELTAC Topical Report

- By letter dated July 10, 2009 (ML091770210) Operating Reactors (NRR) decided to discontinue review of this report due to the quality and technical issues. References to Operating Reactors should be removed from this report.
  - This should include removal of the N or N+1 redundancy discussion in the GDC 21 reference.

MELTAC Topical Report

- The identification, and method of such, of the documents and equipment shall meet the requirement of IEEE 603, Criteria 5.11 and, as referenced, IEEE Std 384, 420 and 494 (RAI-05 and Supplement).
- IEEE 603 Criteria 5.11 states “The associated documentation *shall be distinctly identified in accordance with the requirements* of IEEE Std **494.**”
  - Method of identifying safety related documents and documents with portions of safety related information is very explicit in IEEE 494.

MELTAC Topical Report

- The Engineering tool –
  - Temporary or Permanent Connection ? Currently the topical report states temporary:
    - 4.1.4.2; The Engineering Tool, which runs on a Personal Computer, is temporarily connected via the Maintenance Network.
    - 4.5.2; The Engineering Tool is normally not connected to the Maintenance Network.

MELTAC Topical Report

- The Engineering tool –
  - Unidirectional or Bidirectional ?
  - Currently the MELTAC topical report states:
    - When the Controllers are in service (i.e.. not declared inoperable by Technical Specifications) they provide only *unidirectional* *outbound* communication to the Engineering Tool (i.e.. there is no ability for the Engineering Tool to write information to the Controller's memory).

MELTAC Topical Report

- If the topical report is revised to clearly state a
  - Permanent or temporary connection
  - Unidirectional or Bidirectional Communication
- The staff will continue the review beginning with these issues:

MELTAC Topical Report

- ISG 04, Staff Position 1, Point 3
  - Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system.
- ISG 04, Staff Position 1, Point 10, Software enable vs. "Hardwired logic"
- ISG-04, Staff Position 1, Point 12, Communication faults
  - Does there need to be testing to confirm this?

Non-Proprietary

MELTAC Topical Report

- Quality Assurance Program Procedures.
  - Conformance to IEEE software standards reference the (old) Q procedures
  - New procedure changes are not described (Q vs. N)
    - “N” procedures are only in Table 6.3-1 which maps new vs. old documents

MELTAC Topical Report

- Quality Assurance Program Procedures.
  - The staff has reviewed the Q Software Quality Program Procedures.

MELTAC Topical Report

- Quality Assurance Program Procedures.
  - Much of Information for a QAP was not in the Quality Assurance Procedure
  - The staff will provide the RAIs for information until the new document is reviewed by the staff.

MELTAC Topical Report

- Appendix C, Conformance to BTP 7-14.
  - Provides a cross reference from BTP-14, documents and other entities, to the different documents in the QAP
  - Cannot be considered indicative of conformance without the information being submitted on the docket.

MELTAC Topical Report

- Critical Characteristics
  - A commercial grade dedication (CGD) process, as defined in 10CFR21,contains the two major components of CGD:
    - assessment of critical characteristics
    - assessment of built-in quality
  - A list of critical characteristics is not provided in a format conducive to review
  - In other words, there are characteristics throughout the report but not identified as critical characteristics

Software Safety Report

- Provides useful information with regards to ISG-04 review.
- DI&C-ISG-04 contains specific review guidance by which to evaluate the issues in GDC 24, IEEE 603 and IEEE 7-4.3.2. It is a part of the forward process of the life cycle in which the designer ensures that the system does what is intended.

Software Safety Report

- It is suggested that this evaluation be titled as a response to ISG-04 but not titled as a Software Safety Report.
- No reference section is provided;
  - Software Safety Reports should reference:
    - BTP 7-14, Section B.3.1.9, Software Safety Plan
    - RG 1.173, Clause C.3. Software Safety Analysis
    - IEEE 1228, Standard for Software Safety Plans

Software Safety Report

- New structures and buses are mentioned but are not described in the SSR.
- These buses and structures must be described in the hardware architecture for the entire communications system and its hazards to be reviewed.

Software Safety Report

- For the MELTAC platform, the failure modes should be identified and the effects analyzed on module by module basis. The method of hazard identification should be defined.
- Failure effects from the platform level become the failure modes for the system level analysis. The SSR does not identify the platform and application level failures.

Non-Proprietary

Software Program Manuals & BTP 7-14

BTP 7-14 provides information to be reviewed by the staff in the planning, implementation and design output topic areas for software.

- Compliance is not required but identification and analysis of the differences is per 10 CFR 52.47(a)(9).
- 10 CFR 52.47(a)(9) is not referenced in the Safety I&C System & MELTAC Topical Reports or in Chapter 7 of the US-APWR DCD.

Software Program Manuals & BTP 7-14

– Compliance to 10 CFR 52.47(a)(9) with regards to BTP 7-14 was requested in the following RAIs:

- 45 & 56 for the MELTAC Topical;
- 3 (supplemental), 67 and 77 for the Safety I&C Topical
- Question 07.02-2 and the latest set 525-4009 for the US-APWR Design Certification

Software Program Manuals & BTP 7-14

- Any statement in the BTP which includes "should" or "requires" is considered a point of compliance which the staff will review for.
  - This amounts to several hundred statements within the BTP which the staff needs to follow in the review.
  - If an alternative is presented and not analyzed then that is not in compliance with 10 CFR 52.47(a)(9).

Software Program Manuals & BTP 7-14

- The BTP references the six software regulatory guides RG 1.168 – 1.173.
  - Each of these are also stand alone references which apply various IEEE Software Standards.
  - The SPM references only RG 1.169, Configuration Management Plans.

Software Program Manuals & BTP 7-14

- For the six software regulatory guides RG 1.168 – 1.173.
  - Points of review by the staff are the flagged by the words “shall” or “require” as mandatory for the standard; one method as described by the Regulatory Guide.

Software Program Manuals & BTP 7-14

- For the US-APWR Technical Report, MUAP-07017, Software Program Manual.
  - Staff provided 29 questions using BTP-14 based on common issues with other Software Program Manuals
  - Also, the supplemental set, from the Oct 09' meeting is being reviewed.

Software Program Manuals & BTP 7-14

- For the MELTAC Topical Report:
  - The information provided in Section 6.4, BTP 7-14 Assessment, or Appendix C, Conformance to BTP 7-14, does not provide the level of detail, and therefore, does not comply with the information presented in BTP 7-14. At this time, the staff cannot make a safety determination on the basic Software Life Cycle.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Software Program Manuals & BTP 7-14

- For the US-APWR Technical Report, MUAP-07017, Software Program Manual:
  – The information provided does not provide the level of detail, and therefore, does not comply with the information presented in BTP 7-14. At this time, the staff cannot make a safety determination on the application Software Life Cycle as described in this document.

Non-Proprietary

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Software Program Manuals & BTP 7-14

- "In regard to the level of detail required in the applications for design certification and reflected as necessary in ITAAC, the staff should assure that it has all the details necessary to make the final safety decisions on the underlying design- not the functions. **Commitments to meet regulations are not substitutes for details of designs which meet those regulations.**" – SRM SECY-91-178

DCD Review Issues

- The preceding issues on the reports and how they are resolved will have a major impact on the evaluation of the DCD and the design certification for Chapter 7.

- If the base issues in the report is not resolved, the problem may impact the DCD by additional ITAAC, or DAC or an open item in Phase 2 of the Design Certification.

DCD Review Issues

- Unlike the topical reports which will have the RAIs, and responses, issued with them in the approved version of the topical report, the DCD will not have the RAIs included in the approval
- The resolved RAIs must have the content included in the next revision of the DCD. Current and future RAIs up to Phase 2, which are not resolved will become open items.

DCD Review Issues

- Common sensing line
  - Not in compliance with ANSI/ISA S67.02.01-1999.
    - Clause 5.1 states “A single process pipe tap to connect process signals for redundant instruments should not be used.”
    - The clause goes on to state that if a single tap cannot be avoided, “Justification shall address the common mode effects of both plugging and breakage.”

DCD Review Issues

- Common sensing line
  - It appears MHI's position that the ANSI/ISA standard and NRC endorsement would have considered the frequency of a LOCA.
  - However, because the regulations are deterministic, the NRC would not have included the LOCA frequency

DCD Review Issues

- Common sensing line
  - MHI is requested to address the supplemental criteria for the instrument sensing lines provided in RG 1.151 in the endorsement of ANSI/ISA S67.02.

DCD Review Issues

US-APWR
Instrument Setpoint Methodology
MUAP-09022